Using Technology Control Plans in Export Compliance

Mary Beran, Georgia Tech
David Brady, Virginia Tech
What is a Technology Control Plan (TCP)?

• The purpose of a TCP is to control the access and dissemination of export controlled information, materials, technology, data, etc. in accordance with federal export regulations.

• TCP ensures that everyone working on project understand their obligations under the export control laws and regulations.
Authority: TCP Required

• The National Industrial Security Program Operating Manual (NISPOM) 10-509 specifies: “A Technology Control Plan is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities unless the CSA [Cognizant Security Agency] determines that procedures already in place at the contractor’s facility are adequate. The TCP shall contain procedures to control access for all export-controlled information.” (Emphasis Added)

• International Traffic in Arms Regulations (ITAR) 22CFR §126.13 (c) also encourages use of a Technology Control Plan (TCP): “In cases when foreign nationals are employed at or assigned to security-cleared facilities, provision by the applicant of a Technology Control Plan (available from the Defense Investigative Service) will facilitate processing.”
Authority continued

• US Department of Commerce - Export Administration Act (EAA) and EAR Commerce Control List (CCL) -15 CFR §730 -774
• US Department of Energy & Nuclear Regulatory Commission regulations -10 CFR §810, 110, 205
• US Department of the Treasury - Office of Foreign Assets Control (OFAC)
• International Export Regulations & Requirements
• Institutional Policy Requirements
Elements of a Technology Control Plan

• Institutional Commitment
• Commodity jurisdiction and classification
• Physical security
• Information security
• Project personnel requirements
Elements of a Technology Control Plan

• Inspections
• Restricted research training
• Accountability
• Recordkeeping
• Violations and investigations
• Student and Publication Issues
Institutional Commitment

- Required in ITAR Registration
- Required in Voluntary Disclosure submissions
- Recommended key element of Export Compliance Management Plan
Commodity Jurisdiction and Classification

- Determine with sponsor, investigators what is controlled and what is not?
- Determine who has jurisdiction?
- Obtain a CJ if there is doubt
- Document export jurisdiction and classification clearly in the TCP
Commodity Jurisdiction and Classification Best Practices

• If doubt exists-obtain the CJ
  – “ITAR until proven innocent”

• If self classifying:
  – Review USML and 120.3
  – Review contract
  – Discuss with sponsor and PI
  – If not ITAR/DoE, review the CCL
Physical Security
Physical Security Best Practices

• “One lock” principle
• Restricted work area
• Open/closed storage
• Access control and key custody
• Visitor control/ lab tours
• Available guidance
“One Lock Principle”

• There are no regulations specifying required security controls for unclassified export controlled items

• Design physical and IT security to be a minimum of “one lock” away from an inadvertent export without license
  – Passwords, keys, etc.
  – May need multiple locks depending on the items controlled and the foreign persons who may obtain unauthorized access
Restricted Work Area

• When it is necessary to control access to export controlled material in an open area during working hours, a restricted area may be established. A restricted area will normally become necessary when it is impractical or impossible to protect export controlled material because of its size, quantity or other unusual characteristic. The restricted area shall have a clearly defined perimeter, but physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority. [modified from NISPOM 5-305]
Open vs. Closed Storage

- **Closed storage**: the items can be locked in a secure container (cabinet, safe, drawer)
  - preferred (two locks - door and container)

- **Open storage**: the items cannot be stored in a secure container when not in use
  - Less preferred, greater risk of inadvertent violation
  - More security precautions necessary
Access Control and Key Custody

• Access log
• Key control
  – Manual
  – Electronic (preferred)
  – *No piggyback policy!*
• Visitor control
  – Login/logout
  – Escorted
• Third party access control
  (e.g., custodians, maintenance, building mgt)
• Inspection of bags and parcels,
  electronic storage media
Visit Control and Lab Tours

- No visual or oral disclosure of controlled items
- If items cannot be secured during visit - policy of denial when:
  - Deemed export/ defense service risk
  - Not approved by contract or sponsor
  - No need to know
    - DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems (June 12, 2012)
    - Proposed DFAR 252.204-7000 Safeguarding Unclassified Information Rule (June 29, 2011)
- Restricted party & nationality screen
  - Include CV/ Visa review
- Acknowledge TCP and sign NDA
Available Guidance

• DDTC Compliance Program Guidelines
  http://pmddtc.state.gov/compliance/documents/compliance_programs.pdf
• BIS Deemed Exports Webinar
• DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems (June 12, 2012)
• Proposed DFAR 252.204-7000 Safeguarding Unclassified Information Rule (June 29, 2011)
Information Security Best Practices

• NO data storage on personal computers!!!
• NO cloud email exchange or file servers
• NO data storage or backup on shared servers unless approved by Research Security
• NO use of unsecured file sharing programs (sharepoints) unless approved by Research Security
Information Security Best Practices

• Greater security measures for networked machines
• Request that your department IT administrator review the TCP and help setup computers and data storage devices, Research Security can advise
• Basic safeguarding checklist:
  – e.g., antivirus checks, firewall enabled, session lock, audit logs, file encryption
• Strong Passwords:

http://www.awareness.security.vt.edu/passwords/strong_passwords.html
id124061-1
Information Security Best Practices

- Must have dedicated data storage devices (computers/portable hard drives/etc.), these will be “wiped” or dispositioned at conclusion of project
  - Solid state (“flash”) drives must be destroyed, cannot be wiped
  - If portable, must encrypt
- Emails of technical data must be encrypted (PGP, VT Soft Certificate, etc.)
- PI must maintain a list of computers and data storage devices used in the restricted research project, these machines will get higher level security monitoring
Available Guidance

• DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems (June 12, 2012)
• Proposed DFAR 252.204-7000 Safeguarding Unclassified Information Rule (June 29, 2011)
• NIST Special Publications:
  – 800-53 Recommended Security Controls for Federal Information Systems and Organizations
  – 800-88 Guidelines for Media Sanitization
Recordkeeping

• Regulatory requirement vs Institutional Policy:
  – Whichever is longer

• Must be secure storage
  – Coordinate with records management

• Electronic vs paper?

• ITAR Library
Foreign Person Participation

- Must comply with license provisos or terms of license exception/exemption
- Best practices:
  - Make license part of TCP
  - Train all participants (including foreign person) on proviso terms
  - Disclosure of foreign travel
Inspections

- **Kickoff**: Lab or facility inspections are often needed to draft a TCP.
- **Post-award monitoring**: Lab or facility may be inspected as Post Approval Monitoring (PAM) or as part of annual reviews
  - In person vs. via email certification by PI
- **Closeout**: Lab or facility may be inspected as part of project closeout to ensure proper removal or destruction of materials
Personnel Screening

- Restricted Persons Screening (RPS) of all personnel with access to controlled items
- Includes graduate students, undergraduate students, technicians, and IT managers
- Screen individuals and companies
- Many companies offer RPS screening software
  - Dynamic screen
  - State license
Training and Education

• Train all project personnel with access to export controlled items, software or technical data on TCP procedures
• Train all personnel on reporting requirements and possible penalties for noncompliance
• Frequency and type of training may vary:
  – Initial Training vs Refresher
  – In person vs. Online
  – Lab specific vs. Mixed groups
  – Overview (FRE) vs. Specific (EC)
Accountability: Violations & Penalties

Failure to comply with U.S. export control laws can result in severe penalties, both for the individual and institution:

- **Criminal Penalties**
  - Fines: $1,000,000 per violation and imprisonment of up to 10 years.

- **Civil**
  - Fines: $250,000 per violation, or twice the monetary amount of the underlying transaction, which ever is greater
  - If ITAR=$500,000 per violation

- **Debarment**
- **Negative Publicity**

1. ITAR, EAR and OFAC all impose criminal and civil penalties, although the ranges of the penalties vary.
Accountability

• Who is responsible for export compliance under TCP?
• Best
  – Department/PI sign
    • Business manager or IT person for department
  – All persons under the TCP having access to controlled items are required:
    • To take restricted research training
    • sign TCP acknowledgement/ NDA

• Who pays for an export investigation?
Violations and Investigations
Violations and Investigations

• Put procedures in place before a violation occurs

• Specify roles and responsibilities:
  – Legal counsel (inside/outside)
    • Attorney client privilege vs. work product
  – Empowered official(s)
  – Senior management
  – IT support team
  – Faculty, Staff, Students, others involved
  – Other company or institution involved?
Violations and Investigations

- Investigative team “Two-person rule”
- Other company or Institution involved?
  - Heads up and joint VSD
- FOIA issues (state institutions)
- FERPA issues (students)

- Available guidance:
  - SIA Voluntary Disclosure Handbook (May 2010)
Student and Publication Issues

• Issues with student involvement with export controlled items & restricted research:
  – Student record privacy issues
    • FERPA
    • FOIA
  – Risk to student graduation (thesis/dissertation restrictions)
  – Student disciplinary procedures